Glossary

- **Cookie**: When you visit different websites, many of the sites deposit data about your visit, called "cookies," on your computer. Cookies record data such as login information and user preferences.
- **Do Not Track**: A browser-based technology that provides users with a tool to block web advertisers from tracking online behavior.
- **Encryption**: A means of making data unreadable to everyone except the recipient of a message. Encryption is often used to make the transmission of credit card numbers and other personal information secure for those who are shopping on the internet.
- **Geotagging:** The process of adding a location-identifying label to messages, photos, and videos.
- **Phishing**: An identity theft scam in which criminals send out an unsolicited email that often seems to be from a trusted website. The fake messages generally link to websites that request your personal information for authentication purposes. The information, however, goes to the thieves and not to a trusted company.
- **Privacy Policy**: The policy under which the company or organization operating a website handles the personal information collected about visitors to the site. Many website operators publish their privacy policy on their website.
- **Privacy Settings**: Settings within a website that allow users to control what information can be shared with others or remain private.
- **Social Network**: An online community of people who use a website to communicate with each other and share information. Some popular examples include Facebook, MySpace, and Google+.

Resources

For more information, visit the following sites:

- http://ConnectSafely.org: Outlines basic social media safety tips for teens.
- http://www.OnGuardOnline.gov: The Federal Trade Commission provides advice on being safe while using social networking websites.
- https://www.PrivacyRights.org: Provides additional tips on how to use the internet safely, and greater details about the activities that reveal personal information as well as how it is tracked.
- http://www.GetNetWise.org: Resource for looking up internet-related terminology. Also provides tips on how to keep your personal information private through video tutorials and informational links.
- http://StopThinkConnect.org: Provides a roadmap for good online safety practices on computers and mobile phones. Tips are provided in easy to read downloadable PDF files.
- http://www.StaySafeOnline.org: Gives further details on how to maintain a clean machine and to protect personal information when creating passwords, shopping online, or engaging with others on social networks.
- http://www.SaveAndInvest.org: Provides tips on how to help keep your money and identity safe when conducting banking transactions through mobile phones and other portable devices.

Office of Consumer Affairs & Business Regulation
www.mass.gov/consumer

Consumer Hotline:
(617) 973-8787
Toll free: (888) 283-3757

A Brief Guide to

Protecting Your Online Privacy

Office of Consumer Affairs & Business Regulation
Better businesses. Smarter consumers.

Deval L. Patrick
Governor

Barbara Anthony
Undersecretary

Internet Activities That Reveal Personal Data

Did you know that when you are online, you provide information to others? Below is a summary of the more common ways you give information to others when using the internet.

Internet Browsing

Although it may not seem like you are giving very much information when you browse the internet, your browser provides information about which sites you have visited to website operators. As you move from site to site online, many sites embed cookies on your computer to track your behavior.

Search Engines

Most of us navigate the internet by using search engines that can track each search. They are able to identify you, record the search terms you used, the time of your search, and other information.

Social Networks

Information that is shared voluntarily by the user can be gathered and used by advertisers. Such information includes photos, age, gender, status updates, contacts, interests, and geographic location.

Mobile Phones

The above tracking mechanisms also apply when using the internet on your mobile phone.

In addition, many mobile devices track your physical location. Sharing your location tells everyone who is watching where you live or spend time, and when you are not at home.

Managing Privacy on Computers and Mobile Phones

How to opt-out of being tracked online:

Internet Browsers

- Almost all browsers give some control over how much information is kept and stored. Generally, you can change the browser settings to restrict cookies and enhance your privacy.
- Use the following links to increase your privacy when using these popular browsers online:
  - Chrome: www.google.com/intl/en/chrome/browser/features.html#privacy
  - Safari: support.apple.com/kb/PH5000
  - Internet Explorer: windows.microsoft.com/en-us/windows-vista/change-internet-explorer-privacy-settings
  - Firefox: www.support.mozilla.org/en-US/kb/settings-privacy-browsing-history-do-not-track
- In addition, opt out of behavioral advertising delivered by a network of websites by visiting www.networkadvertising.org/choices/

Social Networks

- Be wary about how much personal information you post anywhere online.
- Learn how to use the privacy and security settings.
- Use the following links to manage your privacy within popular social networks:
  - Facebook: www.facebook.com/help/445588775451827/
  - Google +: support.google.com/plus/answer/1047281?hl=en
- Do not post confidential information. What you post may be public by default.

Mobile Phone Tracking

Know your mobile phone's tracking features. To learn how to disable programs and apps from geotagging your location, review your phone instruction manual and the apps' privacy settings.

Protecting Personal Information Online

Practice good online safety habits by following these tips and advice.

Keep a Secure Machine

- Keep security software current.
- Use security software programs to scan your computer and external devices such as USB drives.

Protect Personal Information

- Make passwords more secure by combining capital and lowercase letters with numbers and symbols.
- Use separate passwords for each account.
- Use secure websites that use encryption to protect your personal account information. You can tell a site is secure when it has a lock symbol near the website address or "https:" in the address.
- Set privacy and security settings on websites to limit information sharing.

Connect With Care

If links in emails, tweets, or posts look suspicious, even if you know the source, it is best not to click but instead to delete.

Limit your online behavior while on public Wi-Fi hotspots and adjust the settings on your computer or mobile device to limit who can access your machine.

Identify Scams

Be wary of any communication that suggests you act immediately, offers something that sounds too good to be true, asks for personal information outside of a secure site, or is unsolicited.

The above tips generally apply when using the internet on your mobile phone.